



(11) **EP 0 843 250 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
20.05.1998 Bulletin 1998/21

(51) Int. Cl.⁶: **G06F 1/00, G06F 3/023**

(21) Application number: 97203437.5

(22) Date of filing: 05.11.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 18.11.1996 IE 960815

(71) Applicant:
Alps Electric (Ireland) Ltd.
County Cork (IE)

(72) Inventors:

- McAuliffe, John
Boherbue, Co. Cork (IE)
- Singleton, James
Co. Cork (IE)
- Mlievis, August
3440 Zoutleeuw (BE)

(74) Representative:
Hanna, Peter William Derek et al
Tomkins & Co.,
5 Dartmouth Road
Dublin 6 (IE)

(54) **Computer keyboard with integral encoded device reader**

(57) The present invention relates to a computer keyboard console (1) with an integral encoded device reader, which may for example be a barcode reader, a magnetic card reader or a "smart card" reader or any generally similar device for reading encoded data, for example a personal identification number (PIN) held on the device (3) which may be inserted into a slot (2) defined by the console. The reader comprises an interface in communication with a dedicated microprocessor (17) configured to communicate with means (15,16) for erasably storing or validating data such as security or user identity data, the keyboard matrix circuitry (14), and adapted to communicate with the host computer central processing unit (CPU) (12) via the standard keyboard port connection, and/or via a separate serial connection or interface. Separate reader interfaces may be configured with the dedicated microprocessor to read a barcode device, a magnetic card device, or a smart card device. Means (20,21) are preferably provided to block the communication of said data, when entered via the encoded device reader and/or via user keystrokes on the keyboard, between the keyboard and the host CPU, and preferably to temporarily disable the host CPU - keyboard interconnection or interface until the validation procedure and/or erasure of said data is complete.

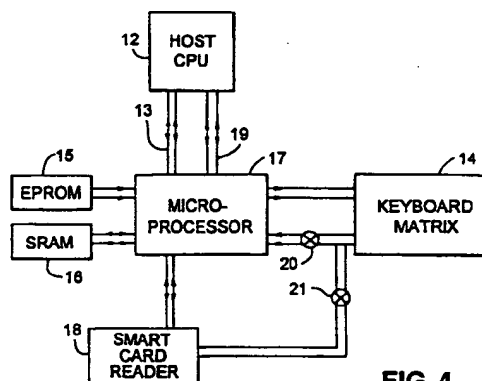


FIG. 4

Description

The present invention relates to a computer keyboard console with an integral encoded device reader, which may for example be a barcode reader, a magnetic card reader or a "smart card" reader or any generally similar device for reading encoded data, for example a personal identification number (PIN) held on the device which may be inserted into the reader.

Separate card reader devices including a smart card reader, for interconnection between a computer keyboard console and a personal computer (PC) have been described in the prior art, for example EP-A-0,486,363 (Thomson-CSF). This describes a smart card read/write unit in a self-contained housing with connections to the computer keyboard and a port on the computer. If specific instructions are entered at the keyboard, data may be read from the smart card and written to the smart card. Numerous devices have been described in the prior art relating to point of sale (POS) devices and automatic cash dispenser machines which may include a key pad and a credit, debit or cash card reader with a magnetic strip including encoded PIN data for communication to a remote computer. However, these are mentioned by way of background only and are not directly relevant to the present invention, which is concerned with a keyboard for a personal computer (PC), network computer (NC), or Internet appliance.

The keyboard console is the standard input device on all personal computers and network computers, and it is particularly in a network environment where security of access by individual users becomes important, i.e. controlling access by certain authorised individuals and restricting access to certain software applications by authorised individuals is an important issue. In order to conduct electronic commerce across a network of computers, such as the Internet, smart cards and similar devices are used for example to transfer "digital cash", to make a credit transfer, or to debit an individual's bank account, and these transactions will increasingly be conducted from a PC or NC with the aid of a card reader device.

A security problem exists with many prior art arrangements in that once encoded data such as PIN data is read from the user's card, whether to initially "unlock" further functionality of the card or to validate data subsequently entered, the PIN details are communicated to a host computer or network server, with the possibility of interception, diversion or corruption. In certain cases, it may not be absolutely necessary to transmit the PIN details to the host, in particular for personal identification purposes and for unloading the card's functionality.

It is an object of the present invention to provide a computer keyboard console with an integral card reader slot, preferably to one side thereof so that the user inserts a card device with encoded data directly into the keyboard.

It is a further object of the present invention to improve the security aspects associated with the transfer of encoded data from the card device to the central processing unit (CPU) of a PC connected to the keyboard, or to a remote computer or network server.

A further object of the present invention is to prevent the transfer of certain encoded data, including PIN data from being communicated to the computer or network, but rather to retain that data locally in the keyboard console device for security and access control applications initiated by normal input from the computer keyboard keys.

According to the present invention there is provided a computer keyboard console including an integral encoded device reader such as a barcode device, a magnetic card device or a smart card device, adapted to be inserted into a slot defined by the console, wherein the reader comprises an interface configured with a dedicated microprocessor in communication with means for erasably storing or validating data such as security or user identity data, and with the keyboard matrix circuitry, and adapted to communicate with the host CPU via the standard keyboard port connection. Said means may be embodied as an erasable programmable read only memory (EPROM), a static random access memory (SRAM), and/or a state machine with no RAM or ROM.

Advantageously, means are provided to block the communication of said data when entered via the encoded device reader and/or via keystrokes on the keyboard between the keyboard and the host CPU. Said blocking means may be provided to temporarily disable the host CPU - keyboard interconnection or interface until the validation and/or erasure of said data is complete. Preferably, when an intelligent encoded data device such as a smart card encoded with a user-defined password is read by the reader and a user is required to enter the password via the keyboard keys to unlock the smart card so that further encoded data may be read by the reader, indicator means on the keyboard is set, and password confirmation is sent directly to the smart card, thereby bypassing the host CPU.

Preferably, separate reader interfaces are configured with the dedicated microprocessor to read different encoded device media selected from a barcode device, a magnetic card device, or a smart card device. Suitably, a cover is provided to cover the slot or slots associated with any redundant reader device not in use.

Preferably, connection with the host CPU is via a universal serial bus interface. Alternatively, an additional serial connection is provided between the dedicated microprocessor and the host CPU.

Preferred embodiments of a computer keyboard console device in accordance with the present invention will now be described with reference to the accompanying drawings in which:

Figure 1 is a perspective view of a standard IBM PC compatible keyboard console including an integral smart card

reader device,

Figure 2 is a block diagram indicating the general configuration of a first embodiment of the present invention including a magnetic card reader and/or a barcode reader,

Figure 3 is a block diagram showing the general configuration of a second embodiment of the present invention, including a smart card reader,

Figure 4 is a block diagram showing the general configuration of a third embodiment of the present invention including a smart card reader with additional security features,

Figure 5 is a block diagram showing the general configuration of a fourth embodiment of the present invention including a smart card reader with additional security features, and

Figure 6 is a block diagram showing the general configuration of a fifth embodiment of the present invention including a smart card reader with additional security features.

Figure 1 shows a standard computer keyboard console 1, but including at the top right corner a slot 2 associated with a smart card 3 reader device forming an integral part of the console. A magnetic card reader device may also be located within the keyboard console and located at the upper right hand side comprising a slot, or at the top left hand side of the keyboard console (not shown) for a manual swipe type reader. A barcode reader socket is internal to the keyboard, but the reader itself may be external, such as a barcode laser scanning device, or a slot may be provided for manual insertion printed barcode cards or other optoelectronic card devices if necessary.

A first embodiment of the present invention includes the integration of a magnetic card reader interface 10 and a barcode reader 11 interface into a keyboard console and is shown in its general configuration in Figure 1. Each device communicates to the host CPU 12 via the keyboard cable 13. The data from each device is converted into standard keyboard codes via the keyboard matrix 14. The integral reader device includes its own EPROM chip 15 and SRAM chip 16 as well as a microprocessor chip 16. The keyboard matrix circuitry, which is standard and need not be described, communicates with the host CPU via the microprocessor and the standard keyboard connection cable 13.

A second embodiment of the present invention is described generally with reference to Figure 3, which is a similar configuration to that described with reference to Figure 2, except that this is a specific configuration to integrate a keyboard and a smart card reader interface 18. The keyboard communicates with the host CPU via the keyboard cable and functions as a normal keyboard. However, in this configuration the smart card reader communicates with the host CPU via a separate serial port cable 19. The smart card acceptor slot 2 is situated at the upper right hand side of the keyboard, as shown in Figure 1.

A third embodiment is shown with reference to Figure 4, and is a specific integration of a keyboard and smart card reader, with additional security features. One of the main features is that when a user is required to enter a password or PIN, the PIN data never leaves the keyboard. When the user specifies a PIN entry mode (for example by hitting a special PIN entry key), the serial interface between the host CPU and the smart card interface is isolated by means of hardware. This is described further with reference to the embodiments shown in Figures 5 and 6. Thus, it is not possible for the host computer or network server to intercept the PIN data by any software means. Communication can be interrupted at one of two points 20,21, between the keyboard matrix/microprocessor link, and/or between the smart card/keyboard matrix link.

The standard numeric key pad section 4 of the keyboard present in all IBM-compatible keyboards, for example, may be modified to incorporate functions for PIN data entry. One possibility is to remove all legends from the key pad except for the numerals, and replace the "NUM LOCK" key legend with "PIN ENTRY" (see key 5, Figure 1) so that the key pad is dedicated to PIN entry. Another option is to assign an additional PIN entry function to the "NUM LOCK" key so that each depression of the key would cause the keyboard to cycle through separate functions, for example from NUM LOCK "on" to NUM LOCK "off" to PIN ENTRY to NUM LOCK "on". An indication that the keyboard is in PIN entry mode may be provided either by a small display mounted on the keyboard, or a dedicated liquid crystal display (LCD) or light emitting diode (LED) 6 for that function.

A fourth embodiment will now be described in more detail with reference to Figure 5. Firstly, connection to the host CPU is via a universal serial bus (USB) interface.

The core security element is that the smart card is locked until a PIN number is validated. In developing the proposed architecture the underlying security principle is that the user, and not the application, controls the switch from "Keyboard Data Mode" to "PIN data mode". To follow this principle the following security criteria may be applied:

- The application requests the user to enter PIN data entry mode.

- The user and only the user can initiate the actions required to enter PIN DATA entry mode.
- The user is informed that the keyboard is in PIN data entry mode by means of a visible indicator or display on the keyboard.
- In PIN data entry mode the keyboard interface to the PC is disabled.
- In PIN data entry mode, the keyboard controller scans the switch matrix and passes keystroke data to the smart card via a ISO7816 interface.
- A "SECURITY SUPERVISOR" State Machine (with no RAM or ROM) controls and monitors the data entry.
- On completion of PIN data entry the keyboard controller undergoes a "warm reset" and all PIN data is removed from the microcontroller memory prior to re-establishing the USB link to the PC.

The following key entry data is supported by the SECURITY SUPERVISOR in PIN DATA ENTRY mode:

Num. Lock [operator confirmation],
0 to 9 numeric keys
DEL. [error correction]
Enter key.

The Security Supervisor implemented as a clock mode sequential circuit (in ASIC) is installed above the 'Normal keyboard functionality' controlling PIN DATA entry through the following steps:

- A: From "the reset state", the PCE-procedure only starts after receiving input from the host via USB-channel.
- B: Start of PCE-procedure to be approved/confirmed by user.
- C: The switching of USB interface lines to Idle state condition for low speed communication devices after (B) and before re-initialisation of all RAM memory.
- D: Outputting via LED indicators / display of clear operator instructions.
- E: State table control as per following sequence:

- 0: State table level
- 1: Reset state PCE-procedure request [after A]
- 2: Secure mode confirmation [after B and C]
- 3: First of 4 PIN-digit entry
- 4: Second of 4 PIN-digit entry
- 5: Third of 4 PIN-digit entry
- 6: Fourth of 4 PIN-digit entry
- 7: End of PCE-procedure [back to reset state]

- F: Warm reset output to the dedicated microprocessor (eg. 8x930x) after end of procedure.
- G: Switching back onto USB interface after completion of warm reset firmware module.

A fifth embodiment will now be described in more detail with reference to Figure 6.

When the device enters "PIN Entry Mode", a separate security module takes control of the switch matrix of the keyboard, so that any key presses are not detected by the keyboard controller. Instead, the matrix scan lines are redirected to the security module, under the control of the security module. The same control at the same time switches the connection between the keyboard controller and the smart card, over to between the security module and the smart card. All communications between the keyboard controller and the security module will be one-way, i.e. from the keyboard controller to the security module, determined by the hardware so that the PIN cannot be passed from the security module to the keyboard controller by a "trap door" or any other means. The security module is embodied as a separate dedicated microprocessor. It should be noted that;

- * A closed switch can be provided on the matrix so the USB controller knows when control of the matrix has been passed back to it from the security module.

* It is possible to add a simple circuit to let the USB microprocessor know when there has been a keypress in PIN Entry mode, without letting it know exactly which key has been pressed.

The following represents a "state table" for the configuration shown in Figure 6.

Host PC	930 USB Controller	Security Module
PIN Entry Request		
	Go into PIN Entry mode	
	Activate PIN Entry control	
	Maintain USB Link & scan matrix to determine when secure mode is complete	Switch into secure mode
		Wait until PIN Entry key is pressed, while PIN Entry mode is active, with timeout
		PIN indicator ON
		Scan matrix & get PIN code
		send PIN to card
		PIN Entry key pressed
		PIN indicator Off
		Switch out of secure mode
	Detect exit from secure mode	
	Send PIN Entry complete to host. Note:- this does not guarantee access to the card, the PIN might be incorrect.	
PC application shall determine whether it has access to the card.		

Physical security is provided by means of a tamper proof label covering one of the keyboard assembly screws so that the user can identify if the keyboard itself has been interfered with.

Additional applications in which a smart card may be used which contains personal data in encrypted form, may include the transmission of encryption keys, the transmission of personal data including medical record data, as well as access control to a network environment, simple boot control may be provided, for example to allow certain users in an office or home environment to boot up a PC, as well as banking and financial applications in electronic commerce, in particular Internet commerce.

Claims

1. A computer keyboard console (1) including an integral encoded device reader such as a barcode device reader (11), a printed barcode card reader, a magnetic card device reader (10) or a smart card device reader (18), wherein the encoded device (3) is adapted to be inserted into a slot (2) defined by the console, characterized in that the reader comprises an interface adjacent said slot configured and in communication with a dedicated microprocessor (17) so as to read encoded data stored on said device, said dedicated microprocessor being configured and in communication with erasable data storage means (15,16) for locally storing, comparing and validating data such as security or user identity data read from said device, said dedicated microprocessor being configured and in communication with the keyboard matrix circuitry (14) for comparing keystroke input data with said stored data, said dedicated microprocessor also being configured and in communication with the host computer central processing unit (12) via the standard keyboard port connection (13), and/or via a separate serial connection (19) or interface.

2. A computer keyboard console according to claim 1, wherein said data storage means comprises an erasable programmable read only memory (EPROM), a static random access memory (SRAM), and/or a state machine with no random access memory (RAM) or read only memory (ROM).
- 5 3. A computer keyboard console according to claim 1 or claim 2, wherein, separate reader interfaces are configured with the dedicated microprocessor (17) to read different encoded device media inserted in the console selected from a barcode device, a printed barcode card, a magnetic card device, or a smart card device.
- 10 4. A computer keyboard console according to any of claims 1 to 3, wherein means are provided to block the communication of said security data, when entered via the encoded device reader and/or via keystrokes on the keyboard, between the keyboard and the host computer central processing unit (12), and preferably said blocking means may be provided to temporarily disable the host computer central processing unit - keyboard interconnection or interface until a validation procedure is complete.
- 15 5. A computer keyboard console according to claim 4, wherein said blocking means comprises means (21) to interrupt communication between said encoded device reader interface and said dedicated microprocessor (17), or means (20) to interrupt communication between said encoded device reader interface and said keyboard matrix circuitry (14).
- 20 6. A computer keyboard console according to claim 4 or claim 5, including an allocated function key (5), the function of which is to signify the commencement of user keystrokes defining security data input.
- 25 7. A computer keyboard console according to claim 4, wherein said blocking means comprises a security module, preferably comprising a separate microprocessor, adapted to temporarily take control of the keyboard matrix circuitry (14) and at the same time switch over the connection between the keyboard matrix circuitry and the encoded device reader (18) to between the security module and the encoded device reader.
- 30 8. A computer keyboard console according to any of claims 4 to 7, wherein means are provided to return control of normal keyboard function to the host computer central processing unit once all security data input to the keyboard console during a given validation procedure has been erased, preferably including a warm reset module.
- 35 9. A computer keyboard console according to any of the preceding claims, wherein said dedicated microprocessor (17) is configured and in communication with the host computer central processing unit (12) via a universal serial bus connection.

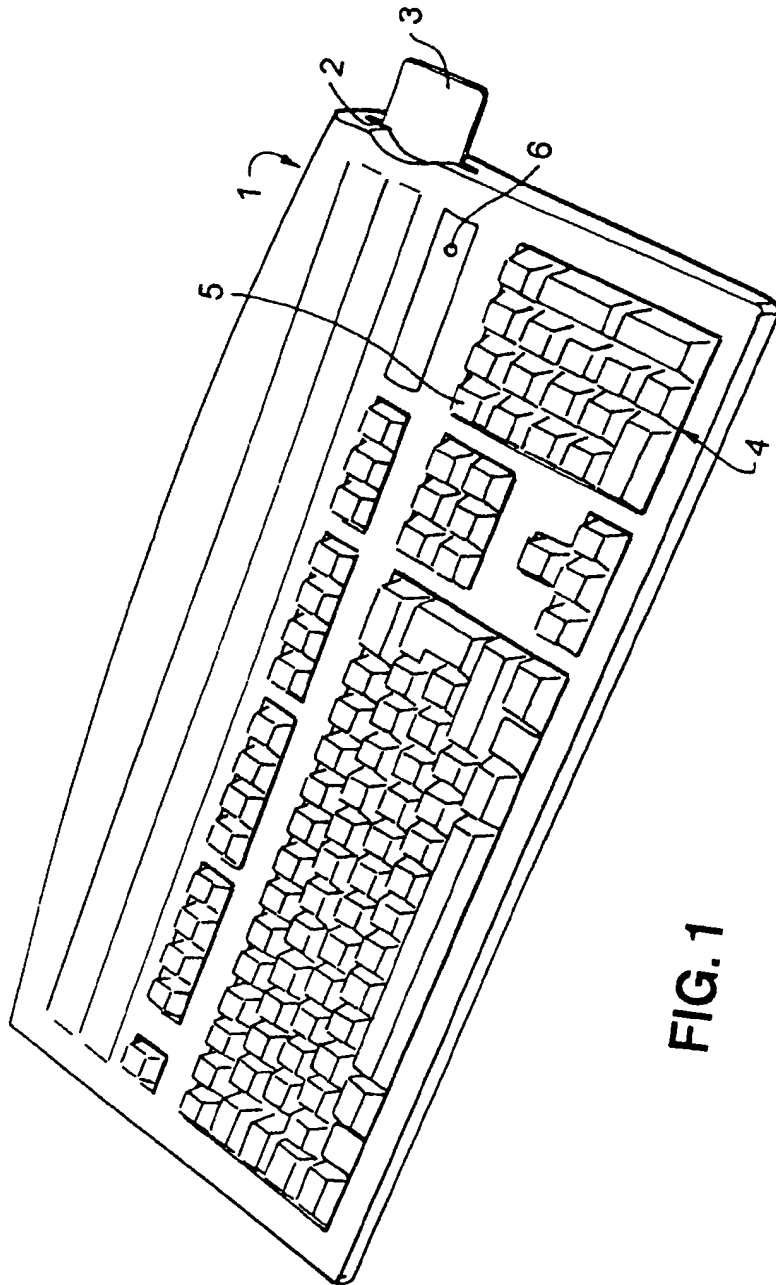


FIG. 1

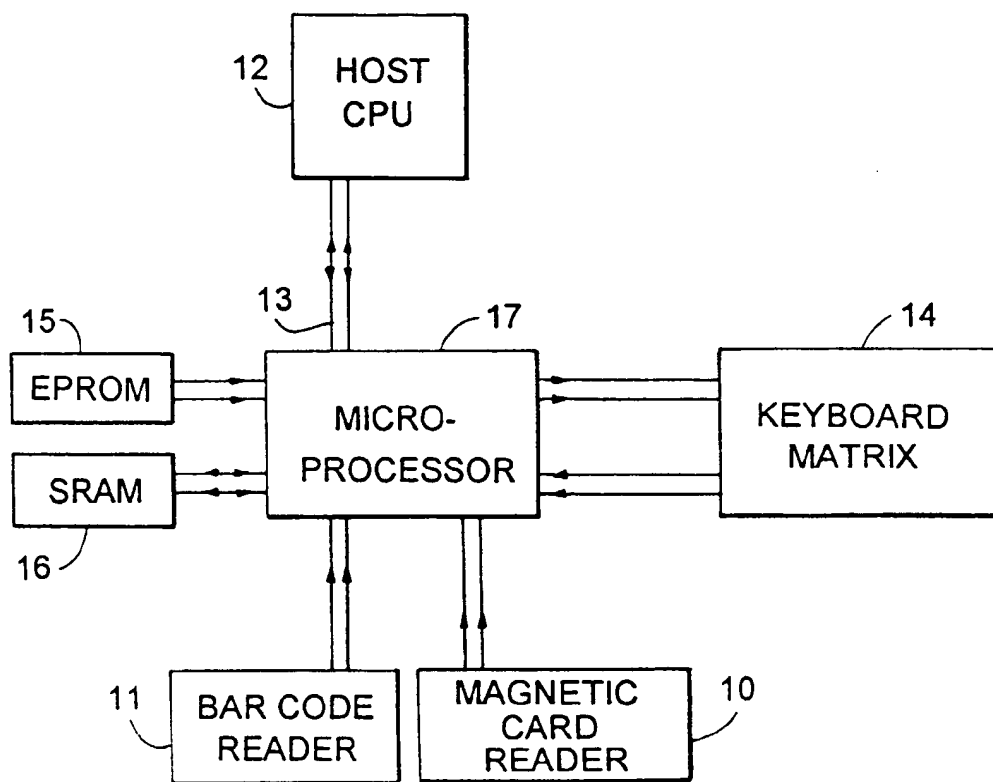


FIG. 2

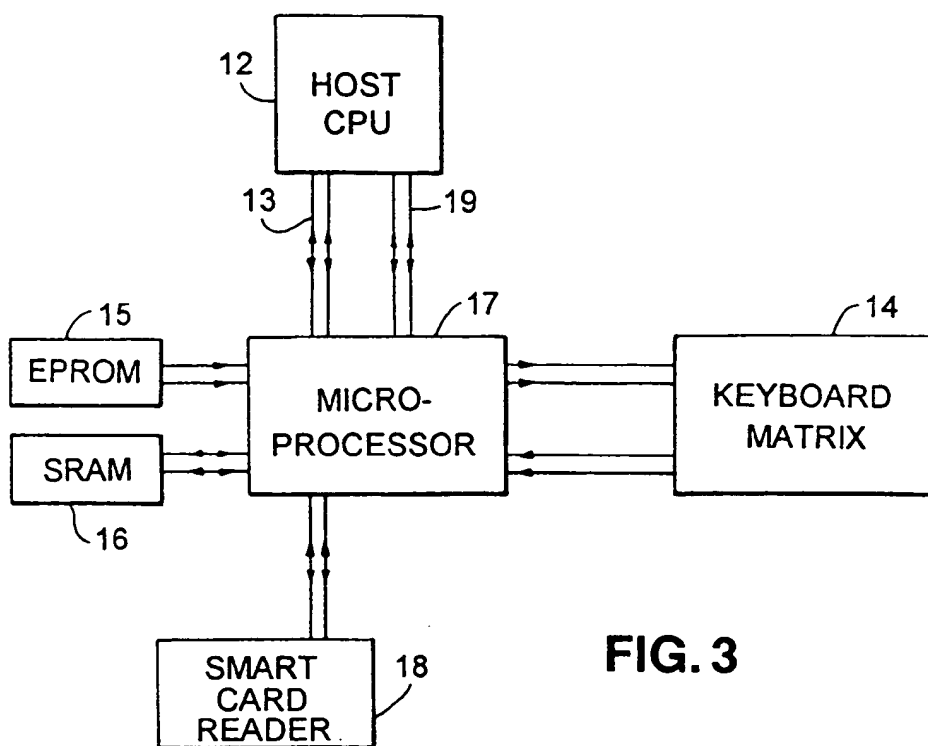


FIG. 3

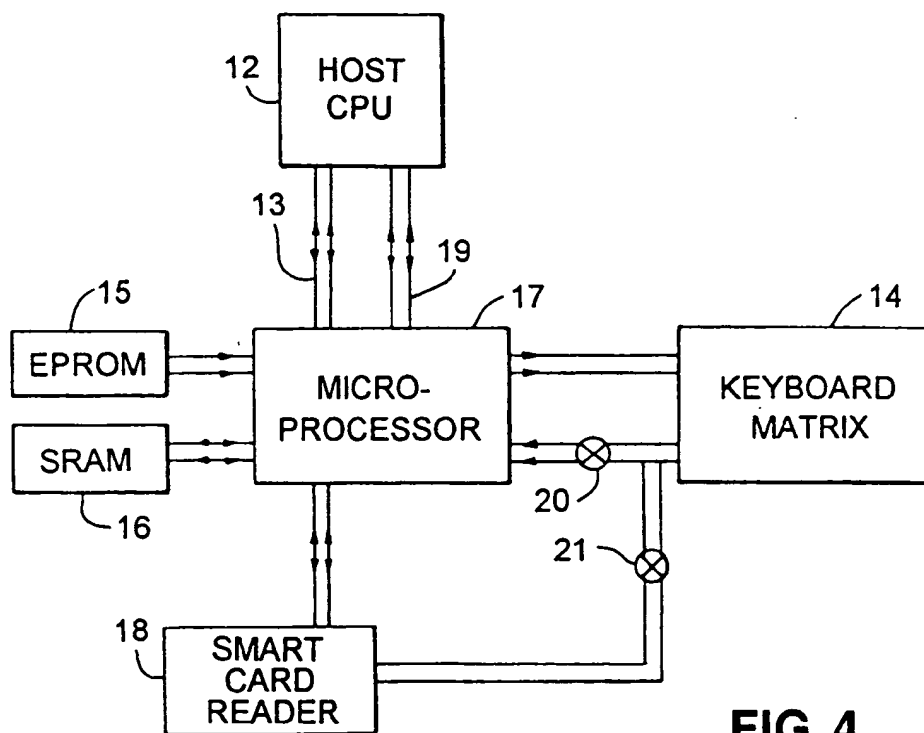


FIG. 4

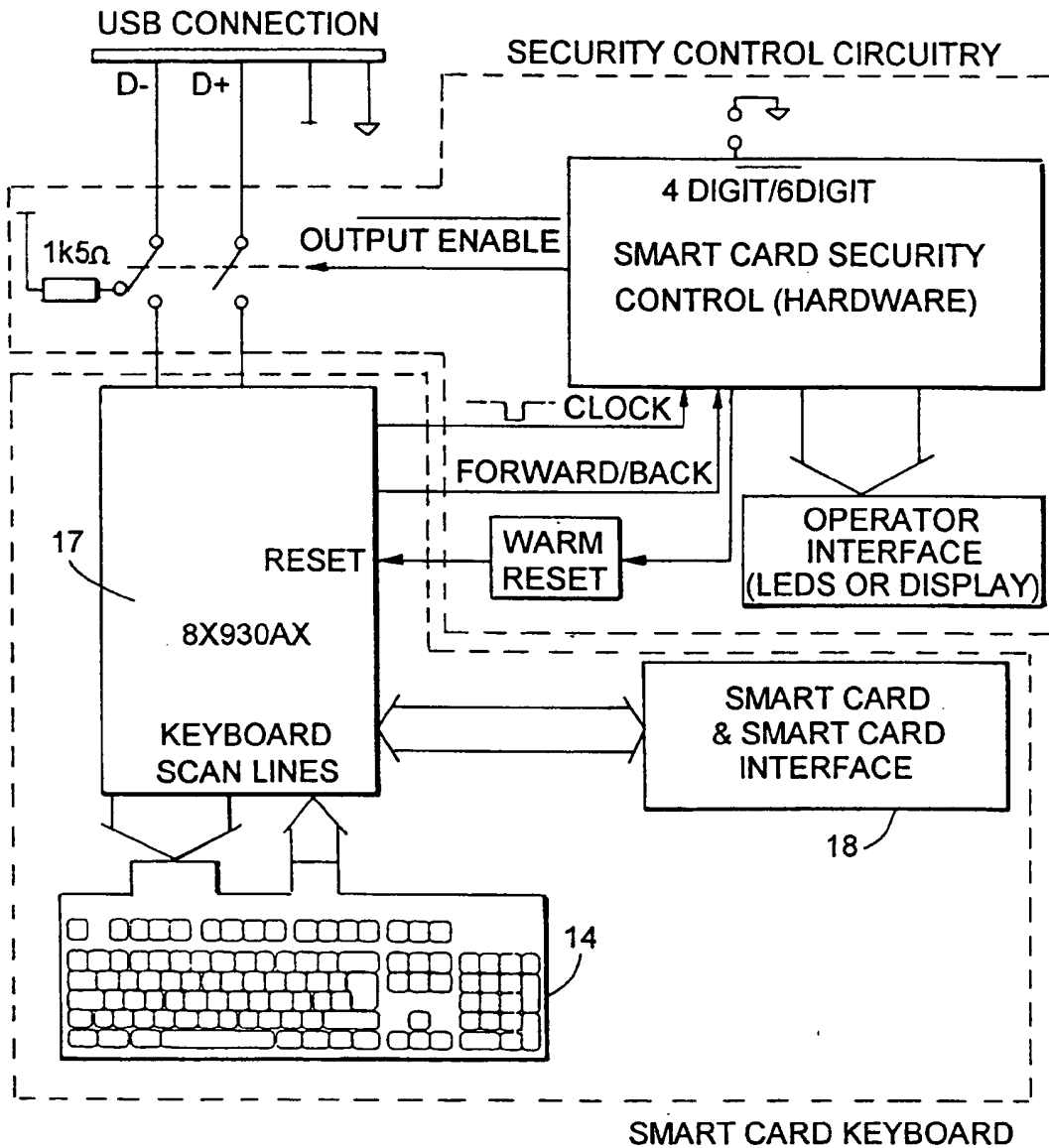


FIG. 5

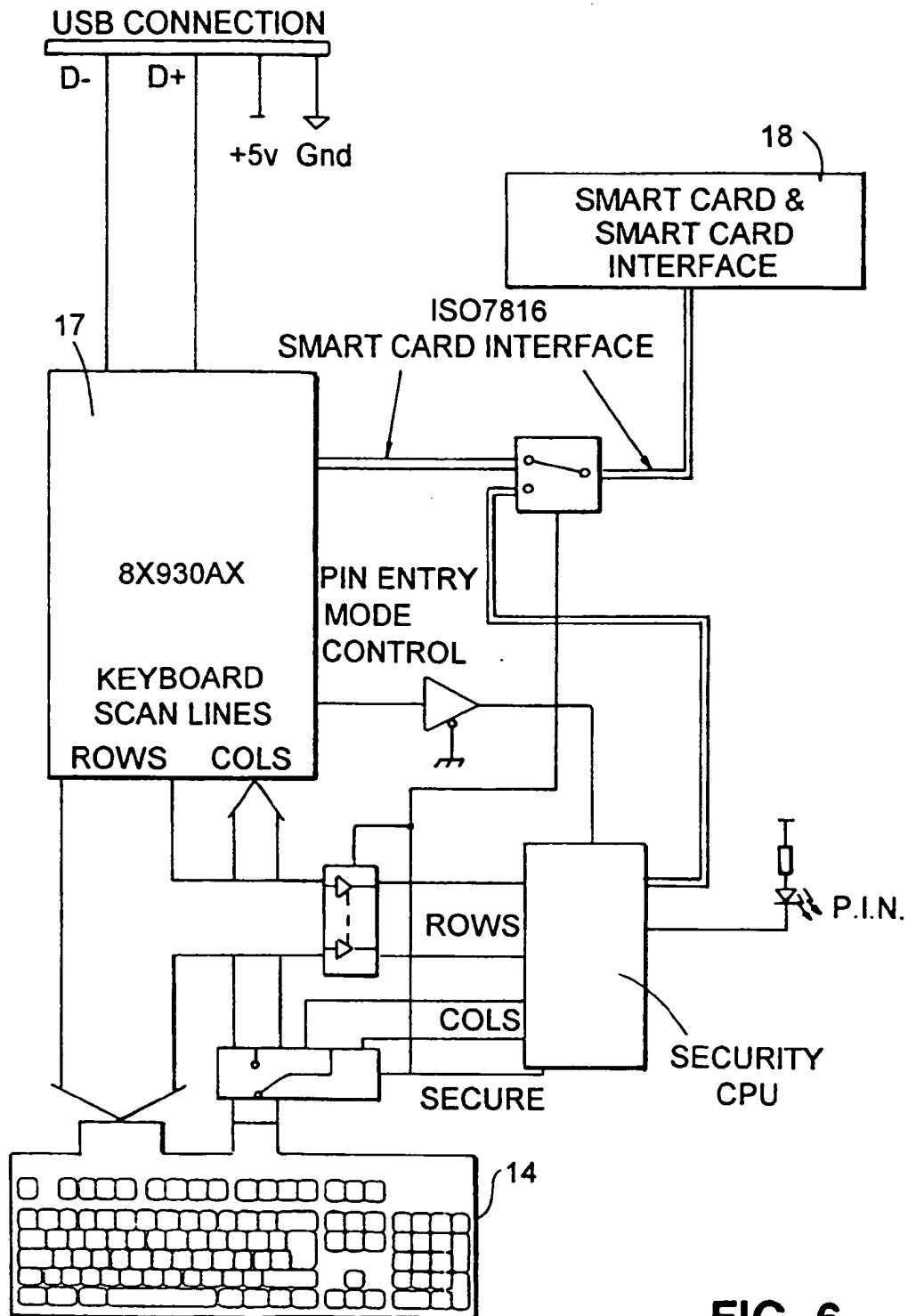


FIG. 6



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 20 3437

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 587 375 A (ALGORITHMIC RES LTD) * abstract * * column 1, line 1 - line 21 * * column 2, line 13 - column 3, line 7 * * column 4, line 14 - column 5, line 55; figure 2 * * column 6, line 54 - column 7, line 12; figure 6 * * column 8, line 5 - line 23 *	1-9	G06F1/00 G06F3/023
A	WO 95 26085 A (INNOVONICS INC ;CLARK DERECK B (US)) * abstract * * page 2, line 27 - line 30 * * page 3, line 1 - line 6 * * page 4, line 33 - line 36 * * page 8, line 6 - line 10 * * page 10, line 3 - line 9; figure 12 * * page 11, line 11 - line 18 * * page 15, line 9 - line 17; figures 14,21 * * page 16, line 13 - page 17, line 2; figure 26 *	1-9	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G06F G07F
P,X	EP 0 763 791 A (HEWLETT PACKARD CO) * abstract * * column 1, line 5 - line 15 * * column 2, line 50 - column 3, line 47 * * column 4, line 38 - column 5, line 19; figures 3,4 * * column 5, line 45 - line 56 * * column 8, line 10 - line 28 * * column 8, line 36 - line 48; figure 6 * * column 9, line 29 - column 10, line 1 *	1-9	
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 4 March 1998	Examiner Bravo, P
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03 82 (P04C01)